融合标签相似度的差分隐私矩阵分解推荐算法 *

郑　剑，王啸乾

(江西理工大学 信息工程学院，江西 赣州 341000)

摘　要：推荐系统需要利用到大量的用户行为数据，这些数据极有可能暴露用户的喜好，给人们关心的隐私问题带来了巨大的挑战。为保证推荐精度与用户隐私，提出一种结合差分隐私与标签信息的矩阵分解推荐模型。该模型首先将标签信息加入到项目相似度的计算过程，随后融入到矩阵分解推荐模型中提高推荐精度，最后运用随机梯度下降法求解模型最优值。为解决用户隐私问题，将拉普拉斯噪声划分成两部分，分别加入项目相似度与梯度求解过程中，使得整个推荐过程满足 ε-差分隐私，并在一个真实的数据集上分析验证算法的有效性。实验表明，提出的方法能在保证用户隐私的情况下，仍具有较高的推荐精度。

关键词：推荐系统；矩阵分解；标签相似度；差分隐私；隐私保护

中图分类号：TP309.2　　doi: 10.19734/j.issn.1001-3695.2018.08.0654

Differential privacy matrix factorization recommendation algorithm fusing tag similarity

Zheng Jian, Wang Xiaoqian†

(*College of Information Engineering, Jiangxi University of Science & Technology, Ganzhou* Jiangxi 341000, *China*)

Abstract: The recommendation system needs to utilize a large amount of user data, which may expose the user's preferences and pose a huge challenge to the privacy concerns. To ensure the accuracy of recommendation and user privacy, this paper proposed a matrix factorization recommendation model combining differential privacy and tag information. Firstly, the model added the tag information to the process of calculating item similarity, then integrated it into the recommendation model to improve the recommendation accuracy. Finally, this paper solved the model optimal value by the stochastic gradient descent method. For protecting users from privacy threats, the proposed approach divided Laplace noise into two parts, which are added to the process of item similarity and gradient solution respectively, so that the whole recommendation process satisfied the differential privacy, and analyzed the validity of the algorithm on a real data set. Experimental results show that the proposed method has high recommendation accuracy while protecting users' privacy.

Key words: recommendation systems; matrix factorization; tags similarity; differential privacy; privacy preserving

0　引言

协同过滤(collaborative filtering, CF)是最流行的推荐技术之一，通过使用各种数据挖掘或机器学习技术来分析用户的历史行为数据实现个性化推荐的，可进一步分为基于邻域的方法和基于模型的方法[1]。如今互联网快速发展及社交网络的兴起，能从社交网络中挖掘用户属性之间的关系来提高推荐精度[2]。与此同时，标签作为用户对物品的描述，也反映了用户的偏好信息[3]，利用标签进行相似度计算能缓解数据稀疏性问题。

虽然推荐系统能够为用户提供个性化的内容和服务建议，但在推荐过程中却存在着侵犯用户隐私的可能性。收集到的用户信息可能被服务提供方有意或无意的泄露，或服务器收到黑客攻击造成用户信息被窃取等，都会导致用户信息泄露[4]。文献[5]表明，攻击者在已知目标用户一定背景信息的情况下创建出与目标用户具有相同评分的虚假邻居用户，然后通过观察推荐系统的输出结果或者项目相关性列表，可以推断出目标用户的行为历史，甚至是评分信息，这类攻击被称为 K 最近邻(KNN)攻击。通常，协同过滤方法采用某些传统的隐私保护技术，如加密、匿名和扰乱等，其中加密技术采用同态加密对用户评分进行加密，然后根据加密数据计算预测评分，从而保护用户隐私[6]。虽然并不会损失推荐精度，但需要额外的计算成本。由于用户与项目数增多及复杂的加密和解密在计算上的限制，基于加密的方法面临着严重的扩展性问题。Batmaz 等人[7]针对不同的评分类型提出了 8 种不同的隐私保护框架，通过均匀分布或高斯分布来随机扰乱评分，但是由于过大的随机性会大大降低推荐精度，因此隐私控制参数难以控制。

差分隐私[8]首次被 Mcsherry 等人[9]应用到推荐系统，通过向物品协方差矩阵中添加噪声再提交给推荐系统，可对推荐结果施加干扰。Sun 等人[10]设计了两种差分隐私分别适用基于物品的协同过滤和基于用户的协同过滤，通过一定概率对用户取样来构造低敏感度评分矩阵计算项目相似度，从而减少噪声的引入量。Friedman 等人[11]针对矩阵分解推荐模型提出了几种差分隐私噪声添加方法。Hua 等人[10]通过对目标函数进行扰乱，并根据用户划分噪声到目标函数。Zhu 等人[13]针对标签推荐系统提出在对标签聚类的过程中添加噪声以扰乱聚类结果，之后通过指数机制从目标标签所在组选择该标签的隐私标签，最后在每个用户的标签权重中添加拉普拉斯噪声来保护用户隐私。鲜征征等人[14]在 SVD++的基础上基于梯度扰动、基于目标函数扰动和基于输出结果扰动三种 SVD++的隐私保护模型。曹春萍等人[15]虽然在推荐系统中利

收稿日期：2018-08-30；**修回日期：**2018-10-08　　**基金项目：**国家自然科学基金资助项目（61462034）；江西省教育厅科学技术研究项目（GJJ170517）

作者简介：郑剑（1977-），男，湖北武人，副教授，硕导，主要研究方向为基于隐私保护的数据发布、推荐系统等研究（zhengji15@163.com）；王啸乾（1994-），男，湖北武汉人，硕士研究生.主要研究方向为推荐系统，隐私保护.

用差分隐私保护标签数据，实则提出的是一种隐私保护标签聚类算法，忽略了对用户评分的保护。

虽然人们已经提出了多种差分隐私推荐算法，但已有算法没有考虑到标签数据在矩阵分解模型中的应用，因此在面对高维稀疏型数据时依然存在扩展性较差和项目冷启动问题。为此本文提出一种融合标签相似度的差分隐私矩阵分解推荐模型（differential privacy matrix factorization based tag, DPMFBT），并同时保护标签数据和用户评分。模型加入基于标签信息的项目相似度作为正则化项以约束项目潜在特征矩阵，并在项目相似度与模型求解过程中加入拉普拉斯噪声，在保证推荐精度的同时保护用户评分的隐私。

1　相关知识

1.1　矩阵分解

由于矩阵分解[16]准确性和扩展性好、灵活性高而成为协同过滤中一种非常流行且有效的方法。矩阵分解是通过对用户—项目评分矩阵降维，将一个高度稀疏的评分矩阵分解为两个低维矩阵，其中一个矩阵看做是用户潜在特征矩阵，另一个为项目潜在特征矩阵。利用用户特征矩阵和项目特征矩阵的乘积来进一步的预测缺失数据。

假设给定一个 $m\times n$ 的评分矩阵 R，它描述了 m 个用户对 n 个项目的评分。矩阵分解方法试图用分解得到的两个 $m\times d$ 和 $n\times d$ 的低维矩阵 P 和 Q 相乘来逼近评分矩阵 R，使得

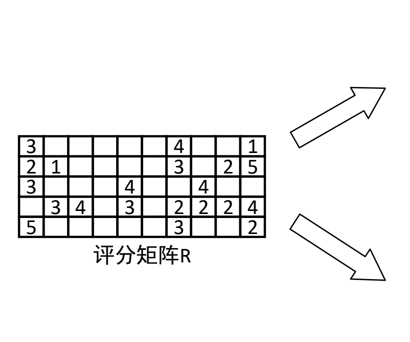
$$R\approx PQ^T \tag{1}$$

其中 $d<\min(m,n)$，矩阵 $P_{m\times d}$ 的第 u 行向量和矩阵 $Q_{n\times d}$ 的第 i 行向量的内积代表着用户 u 对项目 i 的预测评分。

为了使预测评分最贴近用户的真实评分，需最小化矩阵 R 与 PQ 之间的误差。本文用欧氏距离来表示，即

$$\min_{P,Q}\frac{1}{2}\sum_{u=1}^{m}\sum_{i=1}^{n}I_{ui}(R_{ui}-P_uQ_i^T)^2+\frac{\lambda}{2}(\|P\|_F^2+\|Q\|_F^2) \tag{2}$$

其中 I 为指示函数，当用户对项目有评分时函数值为 1，否则为 0。第二项为了防止过拟合，$\lambda>0$ 为惩罚参数，决定目标函数的正则化程度，惩罚参数越大，正则化程度越大。通常采用交替最小二乘法和随机梯度下降法对目标函数进行最小化，求得局部最小值。



3						4			1
2	1					3		2	5
3				4			4		
	3	4		3		2	2	2	4
5						3			2

1.613	-0.065	1.336
1.214	1.740	0.003
1.738	0.273	1.160
0.186	1.623	1.118
0.440	0.703	2.265

0.361	0.888	1.846
-0.507	0.935	1.385
0.995	1.405	1.361
0.979	0.407	0.082
1.237	0.728	1.412
0.089	0.674	0.840
1.791	0.461	0.831
0.084	0.693	0.763
1.395	0.178	1.291
0.709	2.358	0.015

图 1　矩阵分解示意图

Fig. 1　Matrix factorization

1.2　差分隐私

差分隐私是通过添加噪声来掩盖相邻数据集之间查询的差异性。差分隐私查询确保在一个数据集中增加或删除一条数据查询结果保持不变，从而使得攻击者不能根据查询结果推断出用户隐私。并且不需关心攻击者拥有的背景知识，就算攻击者知道除一条记录之外的所有记录信息，也无法推测出这条记录的敏感信息。定义如下：

定义 1　ε−差分隐私[17]。给定一个隐私算法 M，对于两个之多相差一条记录的相邻数据集 D 和 D'，如果算法 M 在这两个数据集上的输出结果 $S(S\subseteq Range(\mathrm{M}))$ 满足下式，则称算法 M 满足 ε−差分隐私。

$$\Pr[\mathrm{M}(D)\in S]\le e^{\varepsilon}\times\Pr[\mathrm{M}(D')\in S] \tag{3}$$

其中：$\Pr[\bullet]$ 代表算法 M 暴露隐私信息的概率；参数 ε 为隐私预算代表隐私保护的程度，一般来说参数值越小隐私保护级别越高，但是会导致查询结果与真实结果偏离较大可用性降低。然而 ε 的取值是一个开放性的问题，它取决于数据拥有方能对用户造成的威胁和用户对隐私的关心程度，有些情况更大的 ε 值可以提供更有意义的隐私保证。

实现 ε−差分隐私的方式主要有两种：拉普拉斯机制和指数机制。前者针对数值型结果，通过向真实查询结果中添加拉普拉斯噪声扰乱查询结果。后者适用于非数值型查询结果，是以一定的概率选择查询结果。噪声的添加量与查询函数的敏感度有关。

定义 2　敏感度[17]。对于查询函数 $f:D\to\mathbb{R}$，相邻数据集 D 和 D'，函数 f 的敏感度定义为

$$\Delta f=\max_{D,D'}\|f(D)-f(D')\|_1 \tag{4}$$

其中：D 和 D' 为至多相差一条记录的数据集。敏感度 Δf 只与查询函数的类型有关，代表着相邻数据集上同一查询结果的最大差异。

定义 3　Laplace 机制[17]。给定数据集 D，对于任意查询函数 $f:D\to\mathbb{R}$，若算法 M 满足式(5)，则该算法提供 ε−差分隐私保护。

$$\mathrm{M}(D)=f(D)+Lap(\frac{\Delta f}{\varepsilon}) \tag{5}$$

Laplace 概率密度函数为 $P(x|b)=(1/2b)e^{(-|x|/b)}$，加入的噪声量与函数的敏感度 Δf 成正比，与隐私预算 ε 成反比。

定义 4　指数机制[18]。假设 $q(D,r)$ 是数据集 D 输出 r 的可用性函数，它度量输出 r 的质量，Δf 表示函数 $q(D,r)$ 的灵敏度，若式(6)成立，则算法 M 满足指数机制 ε−差分隐私。

$$\mathrm{M}(D)=\left(return\ r\propto\exp\left(\frac{\varepsilon q(D,r)}{2\Delta q}\right)\right) \tag{6}$$

1.3　隐私预算的组合性质

一些问题可能需要对隐私预算进行分配后再添加到算法流程中，文献[18]说明了两种得到广泛应用的组合性质：并行组合性和序列组合性。

性质 1　并行组合性。假设有一组隐私机制算法 $M=\{M_1,\ldots,M_m\}$，在一组不相交集上分别满足 ε_i−差分隐私，则组合算法 M 提供 $(\max\{\varepsilon_1,\ldots\varepsilon_m\})$−差分隐私。

性质 2　序列组合性。假设有一组隐私机制算法 $M=\{M_1,\ldots,M_m\}$，在同一个数据集上分别满足 ε_i−差分隐私，则组合算法 M 提供 $(\sum_1^m\varepsilon_i)$−差分隐私。

2　融入标签的隐私保护矩阵分解

2.1　引入标签正则化项的矩阵分解模型

如今社交标签已经成为推荐系统中的一个重要组成部分，用户使用的标签越多代表这个标签对用户越重要，项目被标注某个标签的次数越多则这个标签越能代表这个项目。寻找项目邻居时，在用户评分不足的情况下可以考虑利用标签信息来计算相似度，能够缓解评分数据稀疏性问题。

表 1　项目—标签矩阵

Table 1　Item-tag matrix

	t_1	t_2	…	t_m
i_1	3	10	…	26
i_2	5	21	…	3
…	…	…	…	…
i_n	9	8	…	14

本文用标签向量来表示项目的特征，则项目 i_n 的标签特征向量为 $T_{ni}=(t_{n1},t_{n2},t_{n3},\cdots,t_{nm})$，$m$ 为标签总数，其中每个分量表示项目被标注该标签的次数，项目-标签矩阵如表 1 所示。

用户推荐的项目应该与用户的兴趣越接近越好，因此考虑让每个项目的潜在特征向量与该项目的邻居项目的潜在特征向量更加接近。基于这个假设，在计算项目相似度的时候加入标签信息，从中选择相似度最大的几个项目作为邻居项目并在矩阵分解过程中保持这种联系，因此设计如下基于标签信息的矩阵分解模型(matrix factorization based tag, MFBT)。

$$\min_{P,Q} L(R,P,Q)=\frac{1}{2}\sum_u^m\sum_i^n I_{ui}(R_{ui}-P_uQ_i^T)^2 +\frac{\beta}{2}\sum_i^n\left\|Q_i-\frac{\sum_{f\in N(i)}Sim(i,f)\times Q_f}{\sum_{f\in N(i)}Sim(i,f)}\right\|_F^2 +\frac{\lambda}{2}\left(\|P\|_F^2+\|Q\|_F^2\right) \tag{7}$$

其中：$\alpha>0$，$N(i)$ 表示项目 i 的邻居项目，本文假设在这个模型中每个项目应该与其邻居项目更加接近，并且根据相似度的不同对邻居项目分别对待。在这个目标函数中本文加入了一个正则化项：

$$\frac{\alpha}{2}\sum_i^n\left\|Q_i-\frac{\sum_{f\in N(i)}Sim(i,f)\times Q_f}{\sum_{f\in N(i)}Sim(i,f)}\right\|_F^2 \tag{8}$$

表示项目与其邻居项目的差距，最小化目标函数来使它们之间的差距最小以此来约束项目特征矩阵，使得项目特征向量依据相似度来贴近其邻居项目的特征向量。

2.2　项目相似度计算

为了使得相似度的结果更加准确，本文采用评分信息与标签信息相结合的方式，先根据评分信息利用皮尔逊相关系数计算项目相似度，计算公式如下：

$$Rsim(i,j)=\frac{\sum_{f\in I(i)\cap I(j)}(R_{ui}-\overline{R}_i)\cdot(R_{uj}-\overline{R}_j)}{\sqrt{\sum_{f\in I(i)\cap I(j)}(R_{ui}-\overline{R}_i)^2}\cdot\sqrt{\sum_{f\in I(i)\cap I(j)}(R_{uj}-\overline{R}_j)^2}} \tag{9}$$

其中：R_{ui} 和 R_{uf} 代表用户 u 对项目 i 和项目 f 的评分，$\overline{R_i}$ 和 $\overline{R_f}$ 分别代表项目 i 和项目 f 的平均评分，相似度的取值范围为 $[-1,1]$。然后在利用标签信息计算项目相似度：

$$Tsim(i,j)=\frac{\sum_{f\in I(i)\cap I(j)}(T_{it}-\overline{T}_i)\cdot(T_{jt}-\overline{T}_j)}{\sqrt{\sum_{f\in I(i)\cap I(j)}(T_{it}-\overline{T}_i)^2}\cdot\sqrt{\sum_{f\in I(i)\cap I(j)}(T_{jt}-\overline{T}_j)^2}} \tag{10}$$

其中：T_{ti} 和 T_{tf} 分别代表项目 i 和项目 f 被打上标签 t 的次数，$\overline{T_i}$ 和 $\overline{T_f}$ 分别代表项目 i 和项目 f 的平均标签数。项目 i 与项目 f 的最终相似度为：

$$sim(i,j)=a\cdot Rsim(i,j)+(1-a)\cdot Tsim(i,j) \tag{11}$$

目标函数局部最小值采用随机梯度下降法求得，式(7)对 P_u 和 Q_i 的偏导数如下：

$$\frac{\partial L}{\partial P_u}=\sum_{i=1}^n I_{ij}(P_uQ_i-R_{ui})Q_i+\lambda P_u \tag{12}$$

$$\frac{\partial L}{\partial Q_i}=\sum_{u=1}^m I_{ij}(P_uQ_i^T-R_{ui})P_u+\lambda Q_i +\beta\left(Q_i-\frac{\sum_{f\in N(i)}Sim(i,f)\times Q_f}{\sum_{f\in N(i)}Sim(i,f)}\right) +\beta\sum_{f\in N(i)}\frac{-Sim(i,f)\left(Q_f-\frac{\sum_{g\in N(f)}Sim(f,g)\times Q_g}{\sum_{g\in N(f)}Sim(f,g)}\right)}{\sum_{g\in N(f)}Sim(f,g)} \tag{13}$$

更新方式如下：

$$P_u^{t+1}=P_u^t-\alpha\frac{\partial L}{\partial P_u^t} \tag{14}$$

$$Q_i^{t+1}=Q_i^t-\alpha\frac{\partial L}{\partial Q_i^t} \tag{15}$$

其中：α 为学习速率，代表每次迭代的步长。一般来说学习速率越大迭代次数越少，但是太大会导致迭代结果发散越来越偏离最小值。小学习速率虽然会得到更精确的结果，但是时间代价太大，因此需选择合适的学习速率。

2.3　差分隐私矩阵分解模型

攻击者在已知目标用户一部分项目评分的情况下，如果从推荐系统中得知项目特征矩阵 Q，可通过回归方法推断该目标用户的潜在特征向量，从而获得目标用户对其他项目的评分。本文将拉普拉斯噪声分为两部分，一部分加入到相似度中得到隐私相似度，另一部分加入到梯度求解过程中，使整个矩阵分解过程满足 $\varepsilon-$差分隐私。

2.3.1 隐私相似度

首先对项目的相似度进行隐私保护操作，在相似度计算的过程中加入一部分拉普拉斯噪声来隐藏真实的项目相似度。形式如下：

$$Rsim(i,j)=Rsim(i,j)+Lap(\frac{2\Delta f}{\varepsilon}) \tag{16}$$

$$Tsim(i,j)=Tsim(i,j)+Lap(\frac{2\Delta f}{\varepsilon}) \tag{17}$$

最后根据式(11)计算扰乱后的融合项目相似度，其中敏感度与相似度的计算函数有关，通过式(4)可求得上式中的敏感度值。本文采用的是皮尔逊相关系数，敏感度度则代表皮尔逊相关系数的最大差距，因此可得 $\Delta f=2$。

算法 1 中第 6,7 行分别将拉普拉斯噪声添加到评分相似度与标签相似度中得到各自的隐私相似度，第 10 行以一定权重结合上步得到的两种隐私相似度得到最终的项目隐私相似度。

定理 1　算法 1 满足 $\varepsilon/2-$差分隐私。

证明　对于两个相邻评分矩阵 R 和 R' 及两个相邻的标签矩阵 T 和 T'，由 $Rsim\in[-1,1]$，$Tsim\in[-1,1]$ 它们相似度之间的敏感度分别为：

$$\max\|Rsim_{i,j}(R)-Rsim_{i,j}(R')\|_1=2 \tag{18}$$

$$\max\|Tsim_{i,j}(T)-Tsim_{i,j}(T')\|_1=2 \tag{19}$$

根据差分隐私定理 1，第 6 行与第 7 行添加的噪声满足 Laplace 机制。同时根据差分隐私并行组合性，算法 1 满足 $\varepsilon/2-$差分隐私。

Algorithm 1: Similarity Perturbation

Input: $R=\{r_{ui}\}$ – “user-item” rating matrix;

$T=\{t_{ui}\}$ – “ user-tag” counting matrix;

ε – privacy budget.

Output: $S=\{sim(i,j)\}$ -- privacy item similarity matrix.

1: Divided ε into ε/2 and ε/2

2: **for** each item i **do**

```
    for each item j do
        calculate Rsim(i, j) according to formula (9)
        calculate Tsim(i, j) according to formula (10)
        Rsim(i, j) = Rsim(i, j) + Lap(4/ε)
        Tsim(i, j) = Tsim(i, j) + Lap(4/ε)
    end for
end for
sim(i, j) = a·Rsim(i, j) + (1 − a)·Tsim(i, j)
return S
```

2.3.2 梯度扰乱

本文采用梯度扰乱的方法实现推荐模型的隐私保护。梯度下降的基本思想是以梯度的反方向更新模型从而得到局部最优解，且其幅度与学习速率成比例。梯度扰动方法通过在算法的每次迭代中将拉普拉斯噪声引入梯度下降步骤来保证整个矩阵分解过程中差分隐私机制。另外，可以设置噪声误差以限制噪声的影响，迭代次数 k 是事先已知的，所以每次迭代中引入的噪声可以保持 $\varepsilon/2k-$差分隐私。 k 次迭代保持了 $\varepsilon/2-$差分隐私。

Algorithm 2: private SGD perturbation
Input: $R = \{r_{ui}\}$ – “user-item” rating matrix;
d – number of factors;
α – learning rate parameter;
λ – regularization parameter;
k – number of gradient descent iterations;
e_{max} – upper bound on per-rating error;
ε – privacy parameter.
Output: Latent factor matrices P and Q.

```
1:  Initialize the random latent factor matrices P and Q
2:  for k iterations do
3:      for each r_ui ∈ R do
4:          e' = r_ui − p_u q_i^T + Lap(kΔr/2ε)
5:          e' = { −e_max  if e' < −e_max
                 { e'      if |e'| < e_max
                 { e_max   if e' > e_max
6:      update matrix P according to formula (14)
7:      update matrix Q according to formula (15)
8:  return final P and Q.
```

算法 2 中第 4 行在误差中加入拉普拉斯噪声，并在第 5 行中控制误差在可接受范围内。参数 k 是预设的迭代次数，参数 $\Delta r = r_{\max} - r_{\min}$ 代表最大评分与最小评分的差距。

定理 2　整个矩阵分解过程满足 $\varepsilon-$差分隐私。

证明　对于两个相邻评分矩阵 R 和 R'，由 $e_{ui} = r_{ui} - p_u q_i^T$，评分误差 e_{ui} 的 L_1 敏感度为：

$$\max \| e_{ui}(R) - e_{ui}(R') \|_1 \le \max \| (r - p_u q_i^T) - (r' - p_u q_i^T) \|_1 \le \Delta r \tag{20}$$

根据 Laplace 机制，第 4 行使每次评分都满足 $\varepsilon/2k-$差分隐私。由于迭代的总次数为 k，根据差分隐私的组合性可得求解过程满足 $\varepsilon/2-$差分隐私。

最后，结合定理 2 通过组合性可得整个矩阵分解过程满足 $\varepsilon-$差分隐私机制。

3　实验结果及分析

在本章中，通过具体实验将本文提出的算法应用在真实的数据集上来验证算法的有效性，实验使用 Python 实现相关算法。并将提出的算法和与本文算法相近的文献[3,11,14]进行对比与分析。

3.1　实验数据

本文采用 GroupLens 提供的 MovieLens-1M 数据集。其中包括 700 个用户对 9000 部电影的 100000 条评分记录和用户对电影所标注的 1300 条标签信息。评分范围为 1-5 之间的整数，代表用户的喜爱程度，数值越大越喜欢。数据稀疏度为 98.4%。实验采用交叉验证法将数据集分为 10 组，训练集与测试集的比例为 9:1。

3.2　实验评估指标

本文为评估推荐结果的准确率，采用平均绝对误差(MAE)为评价指标，这个指标越小代表预测准确度越高。其计算公式为

$$MAE = \frac{\sum_{(u,i)\in R} | r_{ui} - \hat{r}_{ui} |}{|R|} \tag{21}$$

其中: $\hat{r}_{ui}$ 代表用户 u 对项目 i 的预测评分， $|R|$ 为评分总数。

3.3　对比算法

将本文提出的差分隐私推荐算法（DPMFBT）、非隐私保护推荐算法（MFBT）分别与五种推荐算法进行比较，验证本文算法的有效性：

a) 与基于标签的用户最近邻推荐(TOCF)对比，验证同样加入标签信息的情况下本文算法的有效性。

b) 与 SVD++进行对比，验证在矩阵分解中将标签相似度作为正则化项的有效性。

c) 与传统梯度扰乱矩阵分解(PSGD)对比，验证在差分隐私矩阵分解下加入标签隐私相似度的有效性。

d) 与 ALS 输出加扰矩阵分解(PALS)对比，验证在差分隐私矩阵分解下加入标签隐私相似度的有效性。

e) 与基于梯度扰动的 SVD++隐私保护(DPSS++)对比，比较标签信息与其他隐式反馈在矩阵分解中关于准确度和噪声敏感度方面的优劣。

算法 1 在基于用户的协同过滤中整合标签信息，利用标签来选择用户的扩展最近邻居填充用户相似度矩阵以降低数据稀疏性。算法 2 在 SVD 的基础上加入隐反馈信息以提高推荐精度。算法 3 为传统矩阵分解的梯度扰动算法。算法 4 为传统交替最小二乘法输出加扰。算法 5 将梯度扰动思想加入到 SVD++推荐方法的求解过程中。

3.4　实验比较与分析

本文实验的参数设置如表 2 所示。

表 2　实验参数设置

Table 2　Experimental parameter setting

变量名	说明	默认值
d	潜在特征向量维度	5
α	学习速率	0.001
λ	惩罚参数	0.01
k	项目邻居数	8
ε	隐私预算	2
β	项目相似度正则化参数	0.01
a	评分相似度权重	0.7
b	标签相似度权重	0.3
e_{max}	评分误差上界	2

实验 1　本文算法与邻域协同过滤算法的对比。

本实验为主要考察不同方法在稀疏数据集上的推荐精确度。将本文提出的 MFBT, DPMFBT 算法与文献[3]基于标签

邻域协同过滤推荐比较，证明本文算法有效性并分析邻居数目对精度的影响。

从图 2 中看出，本文算法明显有着更低的 MAE 值，表明基于模型的协同过滤比基于邻域的协同过滤在稀疏数据上有优势。并且邻居数目 k 的值对推荐结果有明显影响，刚开始推荐精度随着邻居数的增加而减小，在 k=20 时 MAE 达到最小。但当邻居数目继续增长时推荐进度反而会降低，但逐渐趋于平稳，这是因为当选择的邻居较多时，把并不相似的用户和项目纳入到最近邻中从而得到不准确的结果。

实验表明，本文提出的方法拥有更高的推荐精度，并且在加入隐私保护的情况下不会对推荐精度造成很大的损失，仍具有较高的推荐精度。

实验 2　相似度权重对推荐结果的影响。

本实验考察以不同比例融合相似度对推荐结果造成的影响。以用户评分计算出的相似度 a 为横坐标，取值范围为[0,1]，用于观察在不同相似度权重下推荐精度的变化情况。

从图 3 可以看出，当评分相似度权重增大标签相似度权重减小时，非隐私保护推荐算法(MFBT)和带隐私保护的推荐算法(DPMFBT)的 MAE 值都逐渐减少小，当 $a=0.7$ 是达到最低点 0.658(MDBT)和 0.665(DPMFBT)，之后其 MAE 值又逐步上升。当 a 值达到最大值时，两算法的 MAE 值都小于 $a=0$ 时的 MAE 值。因为当 a 值最大时，项目邻居的查找完全依赖于评分相似度，数据中评分数据比标签数据更加密集，因此单纯的评分相似度比标签相似度的邻居质量更高，推荐结果会更准确。

实验表明单一一种相似度都不能得到很准确的推荐，根据评分信息与标签信息的比例适当融合两种相似度可以在一定程度上提高推荐精度。

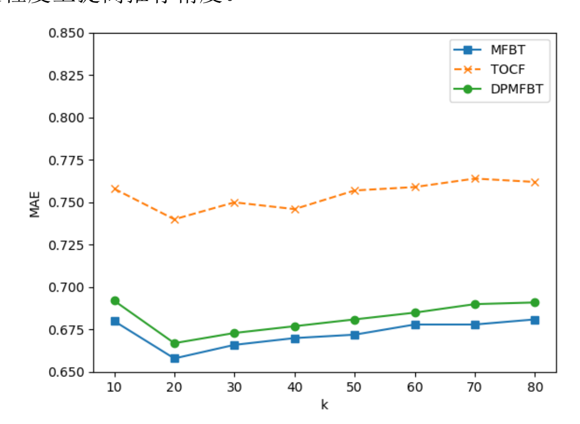


图 2　本文算法与 TOCF 的 MAE 比较

Fig. 2　MAE comparison of proposed algorithms and TOCF

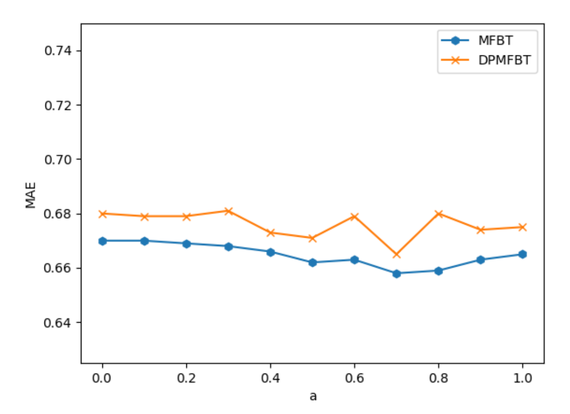


图 3　不同评分相似度权重的 MAE

Fig. 3　MAE of different weight of similarity

实验 3　隐私保护对推荐结果的影响。

本实验意在考察差分隐私对不同算法的影响。因此本文提出的隐私保护推荐算法与文献[14]提出的 DPSS++和文献[11]提出的 PSGD 及 PALS 算法进行对比。观察在不同隐私预算下各算法 MAE 的变化情况。

从图 4 中可以看到推荐算法的 MAE 值随着隐私预算 ε 的增加而降低，这是因为差分隐私的特性，隐私预算越小加入的噪声越多，隐私保护级别也就越高，但是推荐精度会相应地降低。其中 PSGD 与 PALS 算法的 MAE 值最高，变化趋势也最为接近，这是因为这两种方法都只考虑了评分信息，并且这两种算法求解最优值的核心思想相似，因此这两种算法的曲线最为相似。

DPSS++与本文算法 DPMFBT 在评分信息的基础上考虑了隐式反馈和标签信息提高了推荐精度，因此拥有比 PSGD 和 PALS 更低的 MAE 值。同时，可以看出当隐私预算在 1-6 的时候，PSGD 与 PALSMAE 值得变化幅度最大，可断定这两种方法的结果及其依赖于隐私预算的取值，过小的隐私预算会大大破坏数据的可用性。在这一点上，DPSS++与本文算法 DPMFBT 则要好的多，同时没有严重偏离非隐私保护的版本。其中属本文算法最优，不但对噪声的敏感度不高，而且拥有最低的 MAE 值，这是因为本文算法以相似度方式加入标签信息更能表示真实世界的情况，比 DPSS++加入的隐式反馈更加精准明确。

实验表明，本文提出的算法不仅拥有更高的推荐精度，而且在在加入隐私保护噪声的情况下仍具有较高的推荐精度。

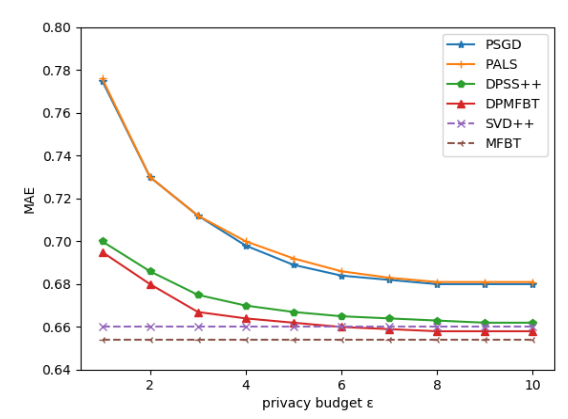


图 4　不同差分隐私参数下的 MAE

Fig. 4　MAE of different privacy budget

实验 4　相似度惩罚参数 β 对推荐结果的影响。

本实验考察参数 β 的变化对本文算法推荐精度的影响，并比较隐私保护版本与非隐私保护版本在 β 变化时的差异。参数 β 在模型中控制加入项目相似度信息的量，在参数 β 极大时，项目相似度则会在模型中占据主要作用；与此相反，当参数 β 极小时，则会削弱项目相似度对项目潜在特征向量的约束，用户-项目评分矩阵开始主导推荐模型。因此参数 β 的选取是一个重要的过程。

可从图 5 中观察到，随着 β 增加即逐渐引入项目相似度信息时 MAE 的值开始减小，在 $\beta=0.01$ 是达到最小值。随着 β 的进一步增大， MAE 的值又开始随着 β 的增加而增大。并且隐私保护算法与费隐私保护算法的变化趋势相同。

实验表明，加入隐私保护后并不会影响推荐结果与用户信息的联系。同时证明了单纯地利用评分信息或标签相似度信息都不能得到准确的推荐结果，只有适当结合着两种信息来源才能获得更准确的推荐。

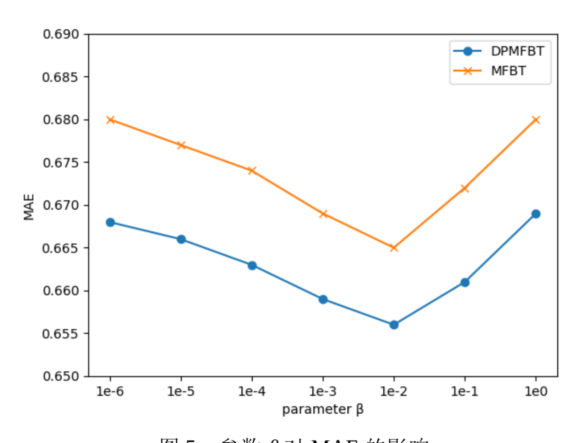


图 5 参数 β 对 MAE 的影响

Fig. 5 Impact of parameter β on MAE

4 结束语

本文以矩阵分解推荐模型为出发点，针对人们所关心的隐私保护问题，将差分隐私应用到矩阵分解推荐模型并结合标签信息，提出了一种融合标签信息的差分隐私推荐模型。在该模型中，利用项目的融合相似度重表示项目潜在特征矩阵，使每个项目特征向量与其邻居的潜在特征向量接近以提高推荐精度，并在相似度与随机梯度下降法的求解过程中添加拉普拉斯噪声，使整个推荐过程满足 ε-差分隐私。通过实验与现有经典算法对比分析，证明了本文提出的算法在保证用户隐私的情况下，能获得与非隐私保护算法相近的推荐精度。但是如何针对不同用户设置隐私保护级别仍是个问题。下一步的研究工作是根据用户关心隐私的程度选取不同的隐私预算参数。

参考文献：

[1] Shi Yue, Larson M, Hanjalic A. Collaborative filtering beyond the user-Item matrix: a survey of the state of the art and future challenges [J]. ACM Computing Surveys, 2014, 47(1): 1-45.

[2] 孟祥武，刘树栋，张玉洁，等.社会化推荐系统研究 [J]. 软件学报，2015, 26(6): 1356-1372. (Meng Xiangwu, Liu Shudong, Zhang Yujie, *et al.* Research on social recommender systems. Journal of Software, 2015, 26(6): 1356-1372.)

[3] 张景龙，黄梦醒，张雨，等. 基于标签优化的协同过滤推荐算法[J]. 计算机应用研究，2018, 35(10)：2916-2919. （Zhang Jinglong, Huang Mengxing, Zhang Yu, *et al.* Collaborative filtering recommendation algorithm based on tag optimization [J]. Application Research of Computers, 2018, 35 (10)：2916-2919.)

[4] Jeckmans A J P, Beye M, Erkin Z, *et al.* Privacy in recommender systems [M]//Social Media Retrieval. London: Springer, 2013: 263-281.

[5] Calandrino J A, Kilzer A, Narayanan A, *et al.* "You might also like: "privacy risks of collaborative filtering [C]// Proc of IEEE Symposium on Security and Privacy. Berkeley: IEEE Press, 2011: 231-246.

[6] Kikuchi H, Kizawa H, Tada M. Privacy-Preserving Collaborative Filtering Schemes [C]// Proc of International Conference on Availability, Reliability and Security. Los Alamos, CA: IEEE Press, 2009: 911-916.

[7] Batmaz Z, Polat H. Randomization-based privacy-preserving frameworks for collaborative filtering [J]. Procedia Computer Science, 2016, 96: 33-42.

[8] Dwork C. Differential privacy: a survey of results [C]// Proc of International Conference on Theory and Applications of models of Computation. Berlin: Springer Press, 2008: 1-19.

[9] Mcsherry F, Mironov I. Differentially private recommender systems: building privacy into the netflix prize contenders [C]// Proc of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM Press, 2009: 627-636.

[10] Zhu Xue, Sun Yuqing. Differential privacy for collaborative filtering recommender algorithm [C]//Proc of ACM on International Workshop on Security and Privacy Analytics. New York: ACM Press, 2016: 9-16.

[11] Friedman A, Berkovsky S, Kaafar M A. A differential privacy framework for matrix factorization recommender systems [J]. User Modeling and User-Adapted Interaction, 2016, 26(5): 1-34.

[12] Hua Jingyu, Xia Chang, Zhong Sheng. Differentially private matrix factorization [C]//Proc of the 24th International Conference on Artificial Intelligence. Austin: AAAI Press. 2015: 1763-1770.

[13] Zhu Tianqing, Li Gang, Zhou Wanlei, *et al.* Privacy-preserving topic model for tagging recommender systems [J]. Knowledge & Information Systems, 2016, 46 (1): 33-58.

[14] 鲜征征,李启良,黄晓宇,等.基于差分隐私和 SVD+的协同过滤算法研究[J/OL].控制与决策，(2017-11-01) [2018-07-07]. https://doi. org/10. 13195/j. kzyjc. 2017. 0961. (Xian Zhengzheng, Li Qiliang, Huang Xiaoyu, *et al.* Collaborative filtering via SVD+with differential privacy [J/OL]. Control and Decision， (2017-11-01) [2018-07-07]. https://doi. org/10. 13195/j. kzyjc. 2017. 0961.)

[15] 曹春萍，徐帮兵. 一种带隐私保护的基于标签的推荐算法研究 [J]. 计算机科学，2017, 44(8): 134-139. (Cao Chunping, Xu Bangbing. Research of privacy-preserving tag-based recommendation algorithm [J]. Computer Science, 2017, 44(8): 134-139.)

[16] Ma Hao, Zhou Dengyong, Liu Chao, *et al.* Recommender systems with social regularization [C]//Proc of the 4th ACM International Conference on Web Search and Data Mining. New York: ACM Press, 2011: 287-296.

[17] Dwork C. A firm foundation for private data analysis [J]. Communications of the ACM, 2011, 54(1): 86-95.

[18] Zhu Tianqing, Li Gang, Zhou Wanlei, *et al.* Differentially private data publishing and analysis: a survey [J]. IEEE Trans on Knowledge & Data Engineering, 2017, 29 (8): 1619-1638.